CLAIMS

What is claimed is

1. A method for secure communications between a client and one of a plurality of servers performed on an intermediary device coupled to the client and said plurality of servers, comprising:

(a) establishing an open communications session between the intermediary device and the client via an open network;

(b) negotiating a secure communications session with the client;

(c) establishing an open communications session with said one of said plurality of servers via a secure network;

(d) receiving encrypted data from the client via the secure communications session;

(e) decrypting encrypted application data;

(f) forwarding decrypted application data to the server via the secure network;

(g) receiving application data from the server via the secure network;

(h) encrypting the application data; and

(i) sending encrypted application data to the client.

2. The method of claim 1 wherein said step (a) comprises the sub steps of:

receiving a request for a communications session from the client;

responding to the request for a communications session in place of the server; and

establishing a secure communications session between the client and the intermediary device.

3. The method of claim 2 wherein said step of (a) comprises receiving a TCP SYN packet from a client and responding to the SYN packet with appropriate responses as a proxy for the server.

4. The method of claim 1 wherein said step of negotiating a secure communications session comprises negotiating an SSL session with the client in place of the server.

5. The method of claim 1 further including the step of authenticating decrypted application data.

6. The method of claim 1 wherein the step of forwarding decrypted application data to said one of said plurality of servers comprises forwarding unauthenticated application data.

7. The method of claim 6 wherein said step of forwarding unauthenticated application data includes the further, subsequent step of authenticating the data

8. The method of claim 1 wherein, prior to said step establishing a communications session with one of said plurality of servers, the method includes the step of:

selecting one of said plurality of servers to forward said decrypted authentication data to based on a load balancing algorithm.

9. The method of claim 8 further including the step of:

tracking data passing between the client and said one of said plurality of servers.

10. The method of claim 9 wherein said step of tracking comprises:

establishing a session tracking database recording, for each session, a session ID, a TCP Sequence number and an SSL session number.

11. The method of claim 10 further including tracking, for each session, an initialization vector.

12. An apparatus coupled to a public network and a secure network, communicating with at least one client via the public network and communicating with one of a plurality of servers via the secure network, comprising:

a network interface communicating with the public network and the secure network;

at least one processor;

programmable dynamic memory addressable by the processor;

a communications channel coupling the processor, memory and network communications interface;

a proxy TCP communications engine;

a proxy SSL communications engine;

a server TCP communications engine; and

a packet data encryption and decryption engine.

13. The apparatus of claim 12 wherein the negotiation manager enables the apparatus as a TCP and SSL proxy for the server.

14. The apparatus of claim 12 further including a load balancing engine to direct application data between the at least one client and said one of said plurality of servers by copying data from an

SSL communications session established by the SSL communications engine to a server TCP session established by the server TCP communications engine.

15. The apparatus of claim 12 wherein the encryption and decryption engine decrypts encrypted packet data to produce application data.

16. The apparatus of claim 12 further including a session tracking database

having at least one record per communication session between the client and server.

17. The apparatus of claim 16 wherein said at least one record includes a TCP sequence number and an SSL sequence number.

18. The apparatus of claim 16 further including a recovery manager using said database to recover from communication errors.

19. The apparatus of claim 12 wherein the packet data encryption and decryption engine decrypts packets from SSL data which spans over multiple TCP segments and forwards packet data to a server which is not authenticated.

20. The apparatus of claim 19 wherein said data is not buffered during decryption.

21. The apparatus of claim 19 wherein said data is buffered for a length sufficient to complete a block cipher used to encrypt the data.

22. The apparatus of claim 20 wherein said packet data encryption and decryption engine includes an authentication process which authenticates the decrypted data after a final segment of a multi-segment encrypted data stream is received.

23. A method of providing secure communications between a plurality of customer devices and an enterprise, comprising:

providing a device enabled for secure communication with customer devices and having an IP address of the enterprise;

receiving communications directed to the enterprise in secure protocol;

decrypting data packets of the secure protocol to provide decrypted packet data;

forwarding the decrypted packet data to at least one server of the enterprise;

receiving application data from a secure server of the enterprise;

encrypting the application data received from the enterprise; and

forwarding encrypted application data to the customer.

24. The method of claim 23 wherein the secure communication is SSL protocol encrypted application data.

25. The method of claim 23 wherein said step of receiving comprises the sub steps of initiating a communications session with the enterprise and negotiating a secure communication session with the device.

26. The method of claim 23 further including the step of negotiating an open communications session with said at least one

server of the enterprise and wherein said step of forwarding includes forwarding decrypted data via the open communications session.

27. The method of claim 23 wherein said step of receiving communications includes receiving a plurality of secure communication sessions from a plurality of customers.

28. The method of claim 27 further including a step of selecting one of a plurality of enterprise servers to which to direct data in said step of forwarding said decrypted packet data.

29. The method of claim 28 further including the step of tracking each communications session between each of said plurality of customers and an associated one of said plurality of enterprise severs.

30. A method for secure communications between a client and one of a plurality of servers performed on an intermediary device coupled to the client and said plurality of servers, comprising:

(a) establishing an open communications session between the intermediary device and the client device via an open network;

(b) negotiating a secure communications session between the intermediary device and the client;

(c) establishing an open communications session between the intermediary device and said one of said plurality of servers via a secure network;

(d) receiving encrypted data from the client via the secure communications session;

(e) decrypting encrypted application data;

(f) forwarding decrypted application data to the server via the secure network;

(g) receiving application data from the server via the secure network;

(h) encrypting the application data;

(i) sending encrypted application data to the client;

(j) detecting a communications anomaly in a communications session between the client and the intermediary device; and

(k) passing TCP data from through the intermediary device.